

UNITED STATES DISTRICT COURT

for the
Eastern District of WisconsinIn the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)Information associated with Amazon Web Services
Account ID:9564 2463 2608; Account ID:956424632608;
and Log on sign in: asupe@seiu105.org

Case No.

14-M-1228

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

located in the Eastern District of Wisconsin, there is now concealed (identify the person or describe the property to be seized):

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

<i>Code Section</i>	<i>Offense Description</i>
Title 18, United States Code Sections 2251, 2252 and 2422 (b)	Production, receipt and possession of child pornography and attempted enticement of a minor to engage in sexual activity.

The application is based on these facts:
See Attached Affidavit

- ☒ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.



Applicant's signature

Kevin Wrona, Dept. of Homeland Security Special Agent

Printed name and title

Sworn to before me and signed in my presence.

Date:

5/30/14 @ 11:44 a.m.



Judge's signature

City and state: Milwaukee, Wisconsin

William E. Duffin, U.S. Magistrate Judge

Printed name and title

AFFIDAVIT IN SUPPORT OF APPLICATION FOR SEARCH WARRANT

I, Kevin C. Wrona, a Special Agent with the Department of Homeland Security, Homeland Security Investigations, Milwaukee Resident Office, being duly sworn, hereby depose and state that the following is true to the best of my information, knowledge, and belief:

INTRODUCTION AND AGENT BACKGROUND

1. I am a Special Agent with the Department of Homeland Security, Homeland Security Investigations (HSI), an investigative branch of the United States Department of Homeland Security. I am a federal law enforcement officer authorized by the Secretary of Homeland Security to request the issuance of criminal complaints and search warrants. As a federal agent, I am authorized to investigate violations of laws of the United States and to execute warrants issued under the authority of the United States. I have been employed as a Special Agent for United States Immigration and Customs Enforcement (ICE), HSI, since June 2010, having previously been employed by Immigration and Naturalization Service (INS) and Customs and Border Protection for the previous seven years. I am currently assigned to the Resident Agent in Charge Office in Milwaukee, Wisconsin. As part of my duties, I investigate criminal violations relating to child exploitation and child pornography, including violations pertaining to the illegal production, distribution, receipt and possession of child pornography, in violation of Title 18, United States Code, Sections 2251, 2252, and 2252A. I have received training and instruction in the field of investigation of child pornography and have had the opportunity to participate in investigations relating to the sexual exploitation of children. As part of my training and experience, I have reviewed images containing child pornography in a variety of formats (such as digital still images and video images) and media (such as storage devices, the Internet, and printed images).
2. I make this affidavit in support of an application for a search warrant for information associated with certain accounts that is stored at premises owned, maintained, controlled, or operated by Amazon.com, Inc., headquartered at 300 Deschutes Way SW, Suite 304, Turnwater, WA 98501. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Amazon.com, Inc. to disclose to the government records and other information in its possession pertaining to the subscriber or customer associated with the accounts, including the contents of communications.
3. Because this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth facts that I believe are necessary to establish probable cause to believe that evidence,

fruits, and instrumentalities of violations of Title 18, United States Code, Sections 2251(a), 2252(a)(4) (B), and 2422(b) are presently located at the Subject Premises.

4. The information contained within the affidavit is based on my training and experience, as well as information imparted to me by other law enforcement officers involved in this investigation.

RELEVANT STATUTES

5. This investigation concerns alleged violations of 18 U.S.C. Sections 2251(a), 2252(a)(4) (B), and 2422(b), relating the sexual exploitation of minors.
6. 18 U.S.C. Section 2252 prohibits a person from knowingly possessing or accessing sexually explicit images (child pornography) with the intent to view them as well as transporting, receiving, distributing or possessing in interstate or foreign commerce, or by using any facility or means of interstate or foreign commerce, any visual depiction of minors engaging in sexually explicit conduct (child pornography).
7. 18 U.S.C. Section 2251(a) prohibits a person from knowingly employing, using, persuading, inducing, enticing, or coercing a minor to engage in any sexually explicit conduct for the purpose of producing any visual depiction of such conduct or for the purpose of transmitting a live visual depiction of such conduct.
8. 18 U.S.C. Section 2422(b) prohibits a person from using the mail or any facility or means of interstate or foreign commerce, including a computer, to knowingly persuade, induce, entice, or coerce a minor to engage in any illegal sexual activity.

DEFINITIONS

9. The following definitions apply to this Affidavit and Attachment B to this Affidavit.
10. "Child Pornography" includes the definition in 18 U.S.C. § 2256(8) (any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct).
11. "Visual depictions" includes prints, copies of visual images, developed and undeveloped film and videotape, and data stored on computer disk or by electronic means, which is capable of conversion into a visual image See 18 U.S.C. § 2256(5).

12. "Child Erotica" means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not, in and of themselves, obscene or that do not necessarily depict minors in sexually explicit poses or positions.
13. "Cloud" and "Cloud Storage" is a model of networked storage where data is stored in virtualized pools of storage which are generally hosted by third parties, which the customers can themselves use to store files or data objects.

INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

14. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require Amazon.com, Inc. to disclose to the government copies of the records and other information (including the content of communications) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.
15. **Amazon.com, Inc** is an online retailer that sells books, DVDs, VHSs, CDs, video and MP3 downloads/streaming, software, video games, electronics, apparel, furniture, food, toys, and jewelry and is a major provider of cloud computing services including cloud storage, Amazon Web Services. Providers like Amazon.com, Inc. ask each of their subscribers to provide certain personal identifying information when registering for an account. This information can include the subscriber's full name, physical address, telephone numbers and other identifiers, e-mail addresses, and, for paying subscribers, a means and source of payment (including any credit or bank account number). Providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (i.e., session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account, and other log files that reflect usage of the account. In addition, providers often have records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the account.
16. In some cases, account users will communicate directly with a provider about issues relating to their account, such as technical problems, billing inquiries, or complaints from other users. Providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well records of any actions taken by the provider or user as a result of the communications.

BACKGROUND REGARDING THE INTERNET AND CHILD EXPLOITATION

17. I have been formally trained in the investigation of crimes involving the sexual exploitation of children. I also own my own computer, have personal knowledge of the operation of a computer, and have accessed the Internet for numerous years. Based on this training and knowledge, and the experience of other law enforcement personnel involved in this investigation, I know the following:
18. The Internet is a worldwide computer network that connects computers and allows communication and the transfer of data and information across state and national boundaries. A user accesses the Internet from a computer network or Internet Service Provider ("ISP") that connects to the Internet. The ISP assigns each user an Internet Protocol ("IP") Address. Each IP address is unique. Every computer or device on the Internet is referenced by a unique IP address the same way every telephone has a unique telephone number. An IP address is a series of four numbers separated by a period, and each number is a whole number between 0 and 255. An example of an IP address is 192.168.10.102. Each time an individual accesses the Internet, the computer from which that individual initiates access is assigned an IP address. A central authority provides each ISP a limited block of IP addresses for use by that ISP's customers or subscribers. Most ISP's employ dynamic IP addressing; that is, they allocate any unused IP address at the time of initiation of an Internet session each time a customer or subscriber accesses the Internet. A dynamic IP address is reserved by an ISP to be shared among a group of computers over a period of time. IP addresses might also be static, if an ISP assigns a user's computer a particular IP address which is used each time the computer accesses the Internet. The ISP logs the date, time and duration of the Internet session for each IP address and can identify the user of that IP address for such a session from these records, depending on the ISP's record retention policies.
19. Child pornographers can now transfer photographs from a camera onto a computer-readable format with a device known as a scanner. With advent of digital cameras, the images can now be transferred directly onto a computer. A device known as a modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Electronic contact can be made to literally millions of computers around the world. The ability to produce child pornography easily, reproduce it inexpensively, and market it anonymously (through electronic communications) has drastically changed the method of distribution and receipt of child pornography. Child pornography can be transferred via electronic mail or through file transfer protocols ("FTP") to anyone with access to a computer and modem. Because of the proliferation of commercial services that provide electronic mail service, chat services (i.e., "Instant Messaging"), and easy access to the Internet, the computer is a preferred method of distribution and receipt of child pornographic materials. Additional Internet-based modes of child pornography distribution and receipt include, but are not limited to, bulletin boards and Internet Relay Chat ("IRC").

A bulletin board is an Internet-based website that is either secured (accessible with a password) or unsecured, and provides members with the ability to view and share postings containing text messages, still images, or web addresses that direct other members to specific content the poster wishes. IRC is a method of communication over the Internet that provides real-time textual messages to be exchanged with a group of users in an IRC channel, or chat room. IRC also provides direct one to one communication using a feature called Direct Client Connection.

20. The Device's capability to store images in digital form makes it an ideal repository for child pornography and other files related to the sexual abuse and exploitation of children. A single compact disk can store dozens of images and hundreds of pages of text. The size of the electronic storage media (commonly referred to as a hard drive) used in home computers has grown tremendously within the last several years. Thumb drives with a capacity of 32 gigabytes are not uncommon. Flash cards with a capacity of 32 gigabytes are not uncommon. Hard drives with the capacity of 500 gigabytes up to 3 terabytes are not uncommon. These drives can store thousands of images at very high resolution. Magnetic storage located in host computers adds another dimension to the equation. It is possible to use a video camera to capture an image, process that image in a computer with video capture capabilities, and save that image to storage in another country. Once this is done, there is no readily apparent evidence at the "scene of the crime". Only with careful laboratory examination of electronic storage devices is it possible to recreate the evidence trail.
21. With Internet access, a user of a Device can transport an image file from the Internet or from another user's computer to his own computer, so that the image file is stored in his Device. The process of transporting an image file to one's own Device is called "downloading". The user can then display the image file on his Device's screen, and can choose to "save" the image on his Device and/or print out a hard copy of the image by using a printer device (such as a laser or inkjet printer). Sometimes the only method to recreate the evidence trail of this behavior is with careful laboratory examination of the Device, modem, printer, and other electronic devices.
22. Your Affiant knows from training and experience that search warrants of residences involved in computer or digitally related criminal activity usually produce items that tend to establish ownership or use of digital devices and ownership or use of any Internet service accounts accessed to obtain child pornography to include credit card bills, telephone bills, correspondence and other identification documents.
23. Your Affiant knows from training and experience that search warrants of residences usually reveal items that tend to show dominion and control of the property searched, to include utility bills, telephone bills, correspondence, rental agreements and other identification documents.

INVESTIGATION

24. On December 20, 2013, Whitefish Bay Police Department (WBPD), Wisconsin, received a report from a resident regarding a possible Internet relationship between her daughter and an adult male from Colorado. On this date, WBPD Detective Joseph McLeod interviewed the Complainant, who informed him that her fifteen-year-old daughter, hereinafter referred to as "Minor Female A", is having an online relationship with a thirty-two year old male from Colorado, who stated his intent to come to visit her daughter over the 2013 winter break. Complainant stated that a friend of Minor Female A, caller Complainant on December 19, 2013, because she was concerned that Minor Female A was involved in an online relationship with an adult male, and has been getting depressed after their conversations. Complainant further stated that the friend of Minor Female A informed a Whitefish Bay Wisconsin High School counselor about this situation. The Whitefish Bay, Wisconsin High School Counselor told the Complainant that the friend of Minor Female A reported to the school that naked pictures have been exchanged between Minor Female A and this man. Complainant stated that she confronted Minor Female A who admitted that she was involved in an online relationship with a thirty-two year old male and that there were plans for him to visit her over the winter break.
25. On December 20, 2013, Detective McLeod interviewed the friend of Minor Female A, who had provided information to the Complainant. This interview took place in the presence of a school counselor. The friend of Minor Female A stated that she came forward to the school counselor and Minor Female A's parents because she was concerned for Minor Female A's welfare. The friend of Minor Female A stated that for the past two months Minor Female A has been distant and depressed due to the online relationship Minor Female A is having with an adult male, whom Minor Female A refers to a "A." The friend of Minor Female A further stated that she believes this man's real name is Andy or Austin, and that Minor Female A has been sad the past two weeks because she and "A" have not been talking. Friend of Minor Female A stated that Minor Female A and "A" met online October 25, 2012, stating she knows this because Minor Female A made a big deal about the date, saying it was their anniversary. The friend of Minor Female A also stated that Minor Female A has sent "A" naked, or partially naked pictures of herself, and that "A" is planning to come to visit Minor Female A during the winter break, expecting to have sex with Minor Female A, but that Minor Female A stated she may not be ready for sex. The friend of Minor Female A described "A" as a white male, tall, bald, with blue eyes, and at least twenty-eight years old. She further believed that "A" was a computer engineer, married, has lots of friends, likes to hike, and has family troubles. The friend of Minor Female A lastly stated that several months prior, Minor Female A stated that she loved "A". Detective McLeod was advised the winter break for the Whitefish Bay High School was scheduled for December 23, 2013, through January 2, 2014.

26. Complainant brought Minor Female A to the WBPD, where she was interviewed by Detective McLeod alone, with the permission of Complainant. Minor Female A identified "A" as Andy M. Supe, stating his birthday is July 18th, and that he was thirty-two years old. Minor Female A defended Supe, saying he has done nothing wrong; that she loves him; and someday they will be together. Minor Female A stated that she met Supe online, on the website "chatroulette.com" where they made a connection, and exchanged personal information. Minor Female A stated she was aware he was thirty-one, and he knew she was fourteen at the time; because she was never deceptive about her age. Minor Female A provided the following information on Supe:

E-mail: andySupe@gmail.com

Skype: Andy S

Cell number: 720-849-9341

27. Minor Female A stated that she has sent Supe naked pictures of herself, and that most of them she had done so on her own. Minor Female A stated that Supe has never sent her any inappropriate picture of himself, but that she has seen his penis on at least two occasions when the two have masturbated with each other over Skype.¹ Minor Female A further stated that she has shown Supe her naked body over Skype. Minor Female A confirmed the plans of Supe to come visit her over winter break, and that the two have discussed having sex when he visits, but that he has stated that he will be patient and wait until she is ready. Minor Female A allowed Detective McLeod to look through her iPhone and he found a photo vault application which contained texts sent between Minor Female A and to Supe. Minor Female A said she saved the text messages because they are important to her, as well as other naked pictures of Minor Female A.

Saved text messages between Supe and Minor Female A include the following:

June 18, 2013

Supe: I love you so completely

Minor Female A: I love you too, sweetheart

Supe: Why would I get bored with you?

Minor Female A: Haha I was mostly giving you murf

Supe: HaHa Sorry if you ever feel pressure, I just know how intimate it will be

¹ Skype is a service which allows users to communicate with others by voice using a microphone, video by using a webcam, and instant messaging over the Internet.

Minor Female A: I have no doubt I'm going to be insanely embarrassed about everything I do at first

Supe: I know, but I will teach you and I am sure you will take pride in it

Minor Female A: I don't want to have to be taught

Supe: Why not? You don't want to learn exactly what I like and dislike?

Minor Female A: Don't take it like that

...

Supe: I know you are willing to try things. I know you love me. Those are huge turn ons too I don't see it as having to teach you I see it as I get to

...

October 16, 2013

Minor Female A sent Supe a naked picture of herself, depicting her breasts and pubic area.

Supe: I love every part of your body, your eyes, your rosy cheeks, your hair your lips your breast, your ass, legs and pussy. Every part of you I am in love with.

28. Complainant also brought Minor Female A's HP laptop to the interview. Minor Female A's HP laptop and iPhone were provided to Detective McLeod and permission was given by Complainant and Minor Female A for forensic examinations to be done on both.
29. Detective McLeod conducted an Accurint search and learned the following information:
Andrew Mark Supe
White Male
SSN: XXX-74-XXXX
17811 E. Iowa Avenue, Aurora, CO 80017
30. Colorado driver's records showed that the license issued to Supe on July 16, 2012, with an address of: 12223 W. 2nd Place, #201, Lakewood, CO 80228.
31. On January 3, 2014, Wisconsin Division of Criminal Investigations (DCI) Special Agents Eric Szatkowski and Tamara Taubel, and DCI Computer Analyst Toby Carlson, responded to the WBPd to do a preliminary forensic examination on Minor Female A's laptop and iPhone. Both items were subsequently released to the DCI agents for a full forensic examination. DCI Agent Szatkowski provided a Colorado Department of Motor Vehicles (DMV) dossier on Supe, which included Supe's photograph.
32. On January 4, 2014, WBPd Officer Hryniewicki met with Complainant and Minor Female A at the WBPd. At that time, Officer Hryniewicki showed Minor Female A two pictures of

Supe, asking if she would be able to positively identify the man in the pictures as Supe. The first picture was a screen shot of the profile picture taken off the Skype account believed to belong to Andy M. Supe. Minor Female A identified the screen capture as belonging to Supe's Skype account, and as the same account that she used to contact Supe. The second photograph was from the Colorado driver's license belonging to Andrew M. Supe. Upon seeing the photo, Minor Female A stated she did not recognize the person. Officer Hryniewicki asked what features she did not recognize, and Minor Female A stated that Supe does not have long hair as in the photo, that he has a full beard instead of a goatee, and that he does not wear glasses. While speaking with Minor Female A's mother, with Minor Female A out of the room, Officer Hryniewicki was informed that Supe has a LinkedIn account as well. Officer Hryniewicki logged into the LinkedIn website and located the page for "Andy Supe," which has the same profile picture as the one used in Supe's Skype account. The LinkedIn account further stated that Supe is a Database Administrator for the SEIU (Service Employees International Union), out of Denver, Colorado, and also provided his e-mail address "andySupe@gmail.com."

33. On January 31, 2014, Detective McLeod received a computer analytical report on Minor Female A's laptop hard drive and her iPhone, from DCI Criminal Analyst Toby Carlson who identified multiple graphic images, as well as Skype chat logs and text message logs. Analysis of the Skype chats by Officer Hryniewicki found the following examples:

09/24/2012 via video chat (lines 1023-1051)

Supe: Haha

Supe: Alright let's see your chest

Supe: You know this goes all the way

Supe: hehe

Minor Female A: ok

Supe: One more layer to go

Supe: You wouldn't accept that from me if I had lost

Supe: No blocking

Minor Female A: whatever

Supe: Fair is fair

Supe: I won fair and square

Supe: You have to hold up your end of the bet

Supe: Very nice

Supe: I like them very much

Minor Female A: can I stop now?

Supe: Nope. I said whole body

Supe: That means pussy too

Supe: You knew that going in
Supe: And if you really hated it you wouldn't be grinning!
Supe: Come lay down, spread your legs
Supe: I said close-up for a reason
Supe: Jennifer, I said close-up for a reason
Minor Female A: no you didn't
Supe: No 5 feet away bs
Supe: Yes I did!
Minor Female A: you said whole body
Supe: I said whole body, close up
Minor Female A: that was close up
Supe: No it was not!

09/28/2012 (lines 2004-2025)

Supe: God I want to see the lips so bad
Minor Female A: I know you do lol
Supe: Please?
Minor Female A: hmmmmm maybe
Supe: :-D
Supe: It'd make my week
Minor Female A: just your week?
Supe: you're right, at least a month
Supe: Seriously
Minor Female A: you sure? i think I look pretty weird down there
Supe: very sure
Minor Female A: Snapshot_20120927_3.jpg
Minor Female A: you asked for it
Supe: Mmmm....looks good to me!

Snapshot_20120927_3 is a photograph of Minor Female A, wearing a white t-shirt, lying on her back, with her legs spread with her hands spreading her vagina apart. Prior to this segment of the chat, Minor Female A had referenced that she is wearing a "t shirt bra and red panties"

12/19/2012 (lines 11639-11654)

Supe: Hey there
Supe: What did you try to send me last night?
Minor Female A: it didn't go through?

Minor Female A: murf.
Supe: Nope
Supe: I can no see
Minor Female A: that'll teach me to try and be sexy haha-it was
some pics of me
Supe: ooooooh really?
Minor Female A: mhm
Supe: You don't happen to have them to send again do you?
Minor Female A: hmmm I might...
Supe: >:-D I would be very appreciative
Minor Female A: haha hang on-uno momento por favor
Supe: k
Minor Female A: Snapshot_20121218.jpg
Minor Female A: Snapshot_20121218_1.jpg

Snapshot_20121218_1 is a photograph of Minor Female A, shot from approximately mid-thigh to just above her breasts. The female is wearing a dark colored bra, and no underwear, with her pubic area completely exposed.

12/19/2012 (lines 11668-11682)

Minor Female A: Snapshot_20121218_4.jpg
Minor Female A: Yes? Or no?
Supe: It worked
Minor Female A: technology! We win!
Minor Female A: Snapshot_20121218_2.jpg

Snapshot_20121218_4 is a photograph of Minor Female A, with brown colored hair who appears to be between the ages of 13-16. She is naked and appears to be lying on her stomach on a bed. She is smiling, and her exposed buttocks are clearly visible.

Snapshot_20121218_2 is a photograph of Minor Female A, who appears to be kneeling. The photo is shot from the side, and is from approximately mid-thigh to just about the breasts. She is naked with part of her pubic area visible, and is partially covering her breast.

03/31/2013 (line 911)

Supe: The fact that you were not born until like 98

06/21/2013 (lines 11510-11519)

Supe: Truth or dare
Minor Female A:dare
Supe: You don't have the guts
Minor Female A: What is it?
Supe: there's no way you'll do it
Minor Female A: Is it to show you my pussy?
Supe: yes
Supe: no playing though, not just kneel and let me see the front
Supe: I want you to lay back and spread your legs.
Supe: I want to see it.
Supe: Minor Female A
Supe: I SWEAR to you, I already know I'm going to like it
Supe: Trust me
Minor Female A: Fine.
Minor Female A: But one condition?
Supe: Which is?
Minor Female A: I take a pic of it later and send it to you?

06/24/2013 (lines 11683-11691)

Minor Female A: I should probably get un-naked soon...or should
we skype/call haha
Supe: How about you stay naked and we skype?
Minor Female A: Sounds good
STARTED_LIVE SESSION
Supe: Hey baby
Minor Female A: Hey yourself
Supe: You're so beautiful

11/08/2013 via video chat (lines 17727-17742)

Supe: well, that means we get to talk more!
Minor Female A: Indeed! AND all the rest of my family is out of the
house so it is nice and peeful
Minor Female A: peaceful
Supe: Oh yeah? All home alone and stuff?
Minor Female A: Yup

Supe: Ooo
Minor Female A: What are you thinking you devilish murf
Supe: That I should go up to my room and we should have a
private show :)
Minor Female A: Really now?
Supe: Yes
Minor Female A: And this would entail....?
Supe: Us both showing off :)
Minor Female A: I see

11/08/2013 via video chat (lines 17762-17781)

Supe: Hey baby
Minor Female A: Hey stranger
Minor Female A: Oh yeah—clothes
Supe: Hehe, yeah
Minor Female A: Well—here goes nothing
Supe: Very nice baby, I just barely can't see your body but very
nice
Minor Female A: that better?
Supe: Yes baby
Supe: You are so hot
Minor Female A: Glad you think so
Supe: I really do baby
Minor Female A: Alrighty
Supe: Can I see that grade A ass of yours?
Minor Female A: Hmm...I suppose
Supe: mmm...I suppose
Minor Female A: Very nice as well
Supe: I wish I was there and inside you right now baby
Minor Female A: Yeah?
Supe: yes

11/08/2013 via video chat (lines 17793-17807)

Supe: I cant wait for us to be together, I want to lick your pussy so
badly
Minor Female A: You definitely ARE craxy
Supe: haha
Minor Female A: Do you want to see it?

Supe: I want to taste you
Supe: yes
Minor Female A: Alright
Supe: Point the camera down and bring it closer
Minor Female A: MM alrighty
Supe: Mmm, yes
Supe: Thoughts?
Minor Female A: It's easier this time
Supe: Does it make it easier that you can see I'm smiling and
hard?
Minor Female A: Yeah
Supe: good

11/08/2013 via video chat (lines 17814-17831)

Supe: okay
Minor Female A: Well...what do I do now?
Supe: Well, we can talk or you could show me something I've never
seen before
Minor Female A: What were you thinking?
Supe: Lay on your stomach your legs nice and wide and using the
other hand on yourself you could show me a lot
Minor Female A: Not sure that would work
Supe: well, if you are on your knees and one hand and using the
other hand on yourself you could show me a lot
Supe: I could pretty much see everything
Minor Female A: I don't know love
Supe: Try for me baby
Minor Female A: Okay I'll try
Supe: Thank you
Minor Female A: I'll have my phone near me so if you can't see just
ext
Minor Female A: text
Supe: ok
Supe: Bring it closer
Supe: You are doing great
Supe: trust me

11/22/2013 (lines 18468-18489)

Supe: So what do you think the chances would be on Christmas
Break

Minor Female A: eh....40% Depending on how easily we could get a
car to get out of Milwaukee..etc

Supe: I can get anywhere

Minor Female A: mmk. I can only get out of the house for maybe 2
days at a time

Minor Female A: I can coordinate with XXX and XXX to make
my parents believe I am with them

Supe: wow, if you could get two days...that'd be amazing!

Supe: I didn't have any expectations of that!

Minor Female A: Well it's be difficult. I'd have to say I was sleeping
over at someone's house, then say I'd be getting a
ride home from them and have either XXX or
XXX verify it

Supe: Yeah

Supe: Well let's NOT plan on that happening

Minor Female A: mmk

Minor Female A: What do you want to plan on happening?

Supe: just us meeting, hanging out, and getting to know one
Another

Supe: if an overnight works easily at the time, great

Minor Female A: how long would you be over here?

Supe: 2-4 days

Minor Female A: mmk

Minor Female A: Sounds good

Supe: I just want to finally meet you and hold you in my arms

Minor Female A: I know baby

Minor Female A: You will

Supe: I so look forward to it

11/25/2013 (lines18689-18704)

Supe: with ONE rule

Minor Female A: Oh boy

Supe: You can guess it if you try I am sure

Minor Female A: I am an idiot, remember?

Supe: I really do want to be the first

Minor Female A: I know

Supe: that's my only real rule

Minor Female A: So basically I can't [expletive] around
Supe: you and I are going to make love dear
Minor Female A: what you just said was "You can [expletive]
around.....except my one rule is you can't [expletive] around"
Supe: oh stop
Minor Female A: It's true
Supe: There's no way, we must make love, I need that with you
baby
Minor Female A: We will
Supe: I'm never leaving you baby :)
Minor Female A: And there's no way anybody else would want me
so you will definitely be the first

12/02/2013 (lines 19867-19878)

Supe: why would I have shame in playing with and loving my
girlfriend?
Minor Female A: Good question
Supe: THAT'S WHY I ASKED IT
Minor Female A: Maybe because she's illegal?
Supe: you're here illegally?
Minor Female A: I'm illegal for you
Supe: [expletive] it
Supe: I don't care
Minor Female A: #jailbait
Supe: truth!
Minor Female A: I'm not even good jailbait! You're terrible at this!
Supe: you'll be the youngest girl I've ever had sex with

12/20/2013 (lines 20099-20106)

Supe: well, this visit will be interesting for sure
Minor Female A: Oh yes. One to remember for sure
Supe: haha, yeah....I hope in a positive way
Minor Female A: Most likely a bit cringe-worthy thought
Minor Female A: though*
Supe: well, we can only do what we can do
Minor Female A: I know, and I know we both will do what we can
Supe: for sure we will my love

34. On February 1, 2014, WBPB Detective McLeod served a State of Wisconsin search warrant on Skype, requesting user, and subscriber information for subscriber: Andy S, with Skype Name: qzgwnxl. On February 14, 2014, Skype responded to the warrant with the following information:

Username: qzgwnxl
Account Creation: 2008-11-10 04:30:16 – UTC
Account Creation IP: 75.70.124.134
Account Creation Country United States
Current E-mail Address: qzgwnxl@hotmail.com
Order Number: 7257000002193424412
Username: qzgwnxl
Order Placed Date: 2013-03-15 – 01:37:25 – UTC
Shopper IP: 98.245.232.26

35. A query of the American Registry for Internet Numbers (“ARIN”) online database revealed that IP address 98.245.232.26 was registered to the Internet Service Provider Comcast Communications and is believed to be located near Aurora, Colorado based on geolocation of the IP address.
36. On March 26, 2014, I served subpoenas to Microsoft Corporation for user information on e-mail address: qzgwnxl@hotmail.com; Google for user information on: andySupe@gmail.com; and Skype for user and subscriber information on: Andy S, and qzgwnxl.
37. On March 28, 2014, I received Google’s response requesting user information on andySupe@gmail.com. The following information was provided:

Name: Andy Supe
e-Mail: andySupe@gmail.com
Secondary e-Mail: qzgwnxl@hotmail.com
Created on: 2010/01/29 – 16:42:28-UTC
SMS: 720-849-9341
Nickname: Andy

The response provided Internet protocol (IP) addresses used, as well as dates and times of login’s between 09/28/2013 and 03/26/2014. One of the IP addresses used was 98.245.232.26, which is the IP address used by Supe to create his Skype account.

38. On April 1, 2014, I served a summons to Comcast Cable Communications, requesting subscriber information on IP address: 98.245.232.26, on 03/23/2014 at 20:57:30 UTC.
39. On April 2, 2014, Comcast provided to me the following on IP address 98.245.232.26, on: 03/23/2014 at 20:57:30 UTC.

Subscriber Name: Andrew Supe
Service Address: 17811 E. Iowa Ave., Aurora, CO 80117-5201
Telephone Number: 720-849-9341
Type of Service: High Speed Internet Service
Account Number: 8497202485540699
Account Status: Active

40. On April 7, 2014, Skype provided to me the following user information:

Username: qzgwnxl
Account Creation Time: 2008-11-10 04:30:16-UTC
Account Creation IP: 75.70.124.134
Account Creation IP Country: United States
Current E-mail Address: qzgwnxl@hotmail.com
Order Placed Date: 2013-03-15 – 01:37:25 – UTC
Shopper IP: 98.245.232.26

41. On April 7, 2014, I, using publically available databases, was able to determine that the address: 17811 E. Iowa Ave., Aurora, Colorado 80017, lists Andrew M. Supe as the resident and owner. The database indicates that the residence was purchased by Supe on January 31, 2013.
42. On April 7, 2014, I advised HSI Denver Special Agent (SA) Shannon Reinert of the above information. SA Reinert contacted the Aurora Police Department who confirmed the address for Supe is the subject premises in Aurora, Colorado.
43. On April 14, 2014, a United States Postal Service Inspector informed HSI SA Reinert that Andrew Supe and two other individuals received mail at the Subject Premises.
44. On April 16, 2014, I swore to a criminal complaint affidavit before the United States District Court for the Eastern District of Wisconsin, and obtained an arrest warrant for Andrew Supe, charging Supe with violations of 18 USC 2422(b) - knowingly used a facility in interstate commerce to knowingly persuade, induce, entice and coerce an individual minor, to engage in sexual activity; and 18 USC 2251(a) – knowingly produced child pornography, in Case No.

14-887 M(NJ). On May 20, 2014, a grand jury sitting in the Eastern District of Wisconsin returned an indictment charging Supe with the same offense. (Case No: 14-CR-113 RTR).

45. On April 22, 2014, I swore out a search warrant affidavit for the premises located at 17811 E. Iowa Avenue, Aurora, Colorado before the United States District Court for the District of Colorado (Case No. 14-sw-05327-BNB).
46. On April 23, 2014, the search warrant for 17811 E. Iowa Avenue, Aurora, Colorado, was executed. At the time of the warrant, Andrew Supe was located at the residence, and was taken into custody pursuant to the arrest warrant. During the search of the residence, numerous items of evidence were recovered, to include computer towers, laptop computers, hard drives, external hard drives, SD cards, CD/DVD's and floppy disks.
47. Two of the computers that were seized belonged to Andrew Supe: an Asus laptop, which was located in Supe's bedroom, and a generic tower computer that contained several hard drives, that was located in the living room.
48. On May 5, 2014, the seized evidence was taken to the HSI Chicago office for forensic examination. Computer Forensic Analyst (CFA) Craig Beebe performed the forensic examination on the electronic devices. CFA Beebe was able to locate chat records between Supe and Minor Female A, as well as pictures of Minor Female A on Supe's Asus laptop computer hard drive and generic tower computer hard drives. CFA Beebe also found remnant evidence on the laptop computer of image files and the names of those files. Several of the file names were the same as child pornography image files that Minor Female A sent to Supe. No images of those files were recovered. However, those files were sent to Supe and accessed on his computers during the fall of 2012 through approximately February of 2013.
49. CFA Beebe was also able to identify nineteen peripheral devices that had been plugged into either the laptop and tower computers (or both), and several of them had been plugged into the computers during the time frame that Supe and Minor Female A were communicating in 2012 and 2013, or shortly before or after that time frame. Some of the devices were plugged into the computers in 2010; however, because Supe engaged in the behavior described in this affidavit over an extended period of time, there is probable cause to believe that he also engaged in the same criminal behavior in 2010. Many of the devices were plugged into the computers while a user logged into the account named "Andy" was using the computers. CFA Beebe explained that in his training and experience, images that are opened on one computer can easily be saved to an external device that is attached to that computer. I also know from my training and experience that those devices can then be attached to other computers and the images on them can easily be saved to those other computers and to other

external devices. I also know that phones, video cameras, and card reader devices, as well as other storage devices can be used to take, store, and transfer images across computers and devices as well as the Internet.

50. The external devices can then be plugged into another computer, such as a work computer, and then their contents can be uploaded to a cloud storage account, such as Amazon's cloud storage service.
51. A review of the forensic report from CFA Beebe revealed that nineteen peripheral devices that had been plugged into either the laptop or tower computer (or both) were not seized during the search warrant. These items include cellphones, USB devices, and video camcorders. These devices are all capable of the storage of electronic media such as pictures, videos, documents, and music.
52. Richard Rosenblatt, attorney for the Service Employees International Union (SEIU), Andrew Supe's employer, provided information that Supe placed unknown data on Amazon's cloud storage service that Supe personally paid for while using his work computer, and that the company wants to cooperate with the investigation. Rosenblatt indicated that Supe's office was on the second floor, east side of the SEIU Local 105 office on 2525 West Alameda Avenue, Denver CO 80219, and that Supe's computer was a Hewlett-Packard HP Pro 3400, Serial Number: I36II6K, Attain Technologies Number: 00I2. Rosenblatt further provided that Supe was using Amazon.com's cloud service, as indicated by the fact that a bill for the service was past due, and that Amazon indicated that they were going to delete the account and its contents unless the bill was paid. Rosenblatt stated that the local union paid the bill on Supe's behalf to keep the account open and its contents available. Rosenblatt provided Supe's account information as: Amazon Web Services: AWS Account ID: 9564 2463 2608; Account ID: 956424632608; Log on Sign in: asupe@seiu105.org.
53. Rosenblatt also provided that other employees reported that Supe brought a laptop to work with him into his office every day. As explained above, it is easy to use external devices to save and move images between computers. Since Supe appears to have brought the same computer to work with him on which law enforcement has found evidence of images of Minor Female A, and Supe's chats with her, there is probable cause to believe that he could likewise have stored external devices in his office, and that he used his work computer and cloud storage to engage in the same criminal activities described above. External devices can be very small and can fit into a desk drawer. In my training and experience, and as explained in more detail below, those who entice minors to self-produce images of child pornography of themselves do not delete those images, but instead keep them in places to which they have access, including offices.

54. Rosenblatt also represented that the contents of Supe's office, computer, and cloud account have not been tampered with or changed in any way since the date of Supe's arrest.
55. Rosenblatt also stated that there is no banner on the workstation computers indication any expectation of privacy in their usage.

**INDIVIDUALS WHO HAVE A SEXUAL INTEREST IN CHILDREN AND PRODUCE
CHILD PORNOGRAPHY**

56. Based on my training and experience related to investigations involving child pornography and the sexual abuse of children, I have learned that individuals who create, possess, receive, distribute or access with intent to view child pornography have a sexual interest in children and in images of children. Based upon my knowledge, experience, and training in child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, there are certain characteristics common to individuals involved in the receipt and collection of child pornography:
- a. The majority of individuals who create and collect child pornography are persons who have a sexual attraction to children. They receive sexual gratification and satisfaction from sexual fantasies fueled by depictions of children that are sexual in nature.
 - b. The majority of individuals who create and collect child pornography collect sexually explicit materials, which may consist of photographs, magazines, motion pictures, video tapes, books, slides, computer graphics or digital or other images for their own sexual gratification. The majority of these individuals also collect child erotica, which may consist of images or text that do not rise to the level of child pornography but which nonetheless fuel their deviant sexual fantasies involving children. Non-pornographic, seemingly innocuous images of minors are often found in email accounts that also contain child pornography, or that is used to communicate with others about sexual activity or interest in children. Such images are useful in attempting to identify actual minors depicted in child pornography images found during the execution of a search warrant. In certain cases, such images may also assist in determining the origins of a particular child pornography image or series of images.
 - c. The majority of individuals who create and collect child pornography rarely, if ever, dispose of their sexually explicit materials and may go to great lengths to conceal and protect from discovery, theft, and damage their collections of illicit materials. They almost always maintain their collections in the privacy and security of their homes, cars, garages, sheds, or other secure storage location, such as on their person.

- d. The majority of individuals who create and collect child pornography often seek out like-minded individuals, either in person or on the Internet, to share information and trade depictions of child pornography and child erotica as a means of gaining status, trust, acceptance and support. This contact helps these individuals to rationalize and validate their deviant sexual interest and associated behavior. The different Internet-based vehicles used by such individuals to communicate with each other include, but are not limited to, e-mail, e-mail groups, bulletin boards, IRC, newsgroups, instant messaging, and other similar vehicles.
- e. The majority of individuals who create and collect child pornography maintain books, magazines, newspapers and other writings, in hard copy or digital medium, on the subject of sexual activities with children, as a way of understanding their own feelings toward children, justifying those feelings and finding comfort for their illicit behavior and desires. Such individuals rarely destroy these materials because of the psychological support they provide.
- f. The majority of individuals who create and collect child pornography often collect, read, copy or maintain names, screen names or nicknames, addresses (including e-mail addresses), phone numbers, or lists of persons who have advertised or otherwise made known in publications and on the Internet that they have similar sexual interests. These contacts are maintained as a means of personal referral, exchange or commercial profit. These names may be maintained in the original medium from which they were derived, in telephone books or notebooks, on computer storage devices, or merely on scraps of paper.

CONCLUSION

57. Based upon the aforementioned factual information, your Affiant respectfully submits this Affidavit in support of probable cause for a Warrant to search the location described in Attachment A, and seize the items described in Attachment B which are in violation of Title 18, United States Code, Sections 2251(a), 2252(a)(4), (B), and 2422(b).

ATTACHMENT A

PROPERTY TO BE SEARCHED

This warrant applies to information associated with Amazon Web Services (AWS) Account ID: 9564 2463 2608; Account ID: 956424632608; and Log on sign in: asupe@seiu105.org that is stored at premises owned, maintained, controlled, or operated by Amazon.com, Inc., a company headquartered at 300 Deschutes Way SW, Suite 304, Turnwater, WA 98501.

ATTACHMENT B

Items to be seized

I. Information to be disclosed by Amazon.com, Inc.

To the extent that the information described in Attachment A is within the possession, custody, or control of **Amazon.com, Inc.**, including any messages, records, files, logs, or information that have been deleted but are still available to **Amazon.com, Inc.** or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), **Amazon.com, Inc.** is required to disclose the following information to the government for each account or identifier listed in Attachment A:

a. The contents of all folders associated with the account, including stored or preserved copies of files sent to and from the account, the source and destination addresses associated with file, and the date and time at which each file was sent;

b. All transactional information of all activity of the **Amazon.com, Inc.** accounts described above, including log files, messaging logs, records of session times and durations, dates and times of connecting, and methods of connecting: and emails “invites” sent or received via Dropbox, and any contact lists.

c. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the types of service utilized, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative e-mail addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

d. All records or other information stored at any time by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, and files;

e. All records pertaining to communications between **Amazon.com, Inc.** and any person regarding the account or identifier, including contacts with support services and records of actions taken.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, evidence and instrumentalities of violations of in violation of Title 18, United States Code, Sections 2251(a), 2252(a)(4), (B), and 2422(b).

III. Method of delivery

Items seized pursuant to this search warrant can be served by sending, on any digital media device, to the Special Agent designated on the fax cover sheet located at the address 790 N. Milwaukee Street, Suite 600, Milwaukee, WI 53202.